NETGEAR®

Business Central Wireless Manager

Data Sheet

Business Central: Your effortless cloud network

Business Central is a secure, cloud based IT service platform designed to provide small to mid-sized organizations with an affordable way to establish, provision and manage key IT networking services. Effortlessly.

Simplify wireless management with anytime, anywhere access directly from the cloud

NETGEAR® Business Central Wireless Manager leverages Software-as-a-Service (SaaS) infrastructure to provide centralized control and comprehensive monitoring of all wireless access points and clients directly from the cloud. With an intuitive user interface and a comprehensive dashboard, Business Central Wireless Manager is the optimum tool for wireless management for small to large enterprises, managed service providers, and organizations with single to multiple branch locations.

Business Central Wireless Manager requires no hardware installation at the customer premise, provides a cost effective pay-as-you-go model, and manages a complete line of ProSAFE® access points. Access is by way of a single sign-on integration with the MyNetgear support portal that provides a single database repository for all NETGEAR products. The same logon credentials are used to access associated Business Central services and allow users access to information about the latest available firmware, FAQ, knowledge database, and customized views for all of the NETGEAR products that the user owns. The need for multiple NETGEAR logins and passwords are eliminated. Centrally hosted with sophisticated load balancing and redundancy, the platform delivers maximum uptime while minimizing capex cost expenditure.

Features

Simplified Management

- Plug and play for ease of access point deployment
- Single Sign-On integration with MyNetgear support portal for complete inventory management
- Anytime, anywhere access for configuration and comprehensive monitoring

Superior Scalability

- Support 100's of thousands of access points and clients
- Centrally hosted in geographically redundant data centers
- Seamlessly manage distributed and remotely located branches and offices

Encrypted Management Architecture

- Separation of management and data traffic to maximize scalability and security
- Secured communication between access points and wireless manager through SSL and certificate validation
- Support VLAN segmentation to ensure maximum security for a variety of user types

Flexible Deployment Model

- Support management of AP's from multiple branch locations behind firewalls
- Optimal solution for retail chains, coffee shops, small offices, multiple branch offices, restaurant chains
- Support management of single or multiple AP's in single or multiple locations

Complete wireless feature set

- Support complete list of wireless security features (WPA, WPA2, AAA)
- Automatically adjust AP parameters by constantly monitoring the RF environment
- Private and public wireless access with complete control and visibility

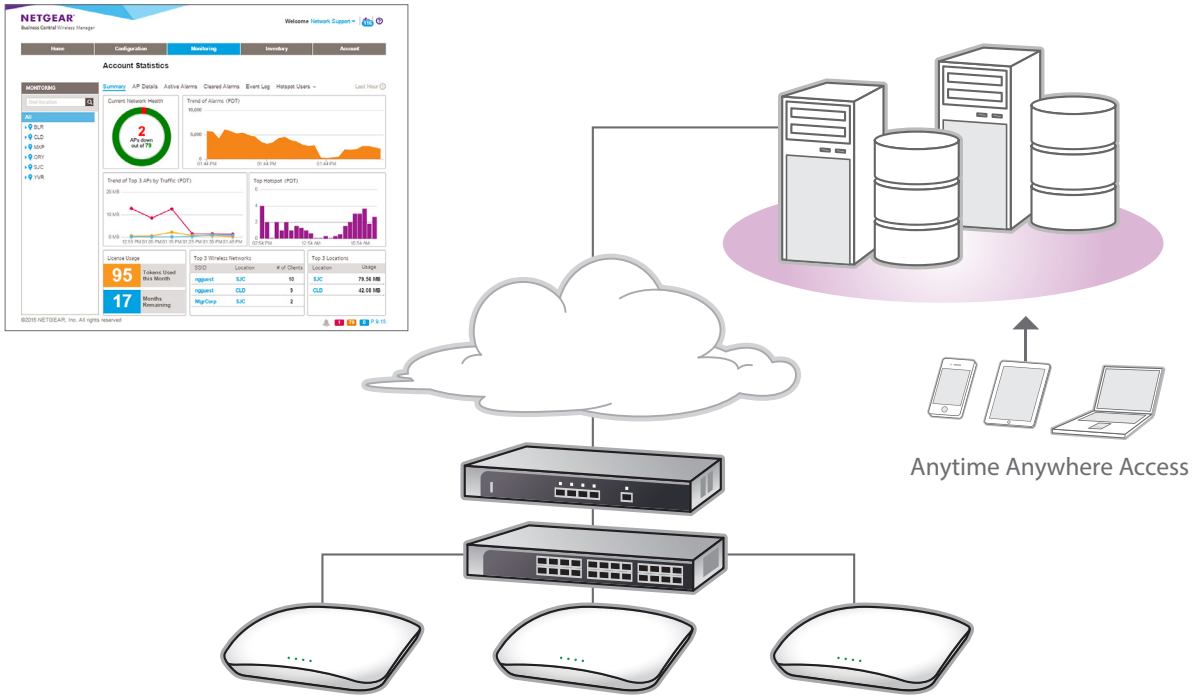
Cost effective solution

- Pay-as-you-go model with cost effective subscription model
- Industry best total cost of ownership for managed access point architecture
- Simple deployment maximizes managed service provider's return on investment
- Create free or chargeable wi-fi hotspots for additional revenue opportunities

BUSINESS CENTRAL

LIFETIME Tech Support

Deployment model for single location



Common use cases for multiple locations

Business Central Wireless Manager.
End user self-managed route

Business Central Wireless Manager.
Managed service provider route

Supported Access Points

Access Points	Description	Part Numbers	Typical Deployment	Product Image (Front)	Product Image (Back)
WNDAP660	ProSAFE Wireless-N Dual Band Concurrent Premium Access Point	WNDAP660-100AUS WNDAP660-100NAS WNDAP660-100PES WNDAP660-100PRS WNDAP660-100UKS	High density, multi-site establishments (restaurants, hotels, coffee shops, retail) for dual band client access		
WNDAP360	ProSAFE Wireless-N Dual Band Concurrent Access Point	WNDAP360-100AJS WNDAP360-100NAS WNDAP360-100PES WNDAP360-100PRS WNDAP360-100UKS	Medium density, multi-site establishments (restaurants, hotels, coffee shops, retail) for dual band client access		
WNDAP350	ProSAFE Wireless-N Dual Band Concurrent Access Point (Metal)	WNDAP350-100AUS WNDAP350-100NAS WNDAP350-100PES WNDAP350-100UKS	Medium density industrial multi-site deployments (ware-house, hardnened locations) for dual band client access		
WNAP320	ProSAFE Wireless-N Single Band Access Point	WNAP320-100AUS WNAP320-100NAS WNAP320-100PES WNAP320-100PRS WNAP320-100UKS	Low density, multi-site establishments (restaurants, hotels, coffee shops, retail) for single band client access		
WNAP210	ProSAFE Wireless-N Single Band Access Point	WNAP210-200AUS WNAP210-200NAS WNAP210-200PES WNAP210-200PRS WNAP210-200UKS	Entry level wireless with minimal density (restaurants, hotels, coffee shops, retail) for single band client access		

Features

Ease of Management

Business Central Wireless Management is performed by remote access through a standard web browser. With an intuitive dashboard and simple to use configuration wizards, the IT administrator can configure and monitor single or multiple access points all with a click of a mouse. Leveraging NETGEAR's best-in-class user experience design, Business Central Wireless Management gives the IT administrators clear and comprehensive status of remote locations, and reduces the operational expenses to manage access points in multiple locations.

Near Limitless Scalability

Business Central Wireless Manager is built on a distributed architecture that does not depend on a centralized controller for either wireless traffic control plane or wireless traffic data plane management. This key differentiating characteristic allows unparalleled scalability of wireless network environments without needing to upgrade or resize a wireless controller. Also, as additional resource is needed, the hosting environment automatically adds resources without the need for users to intervene.

Secured Data Flow

Client traffic is kept entirely on the organization's Local Area Networks. Business Central Wireless Manager only communicates management changes (configuration, setup, administration, and reporting) and traffic monitoring reports for given access points. The Business Central Wireless Manager is out of band from the data path. NETGEAR Business Central Wireless Manager intelligently and securely separates data and controls traffic. While the data traffic remains in the local area network, the cloud management platform handles the control and monitors traffic independently of the data path. Following the model of Software Defined Networking, this distributed model ensures maximum scalability and ease of introducing new features and functionality independent of the access network.

Secured and Private Information Storage

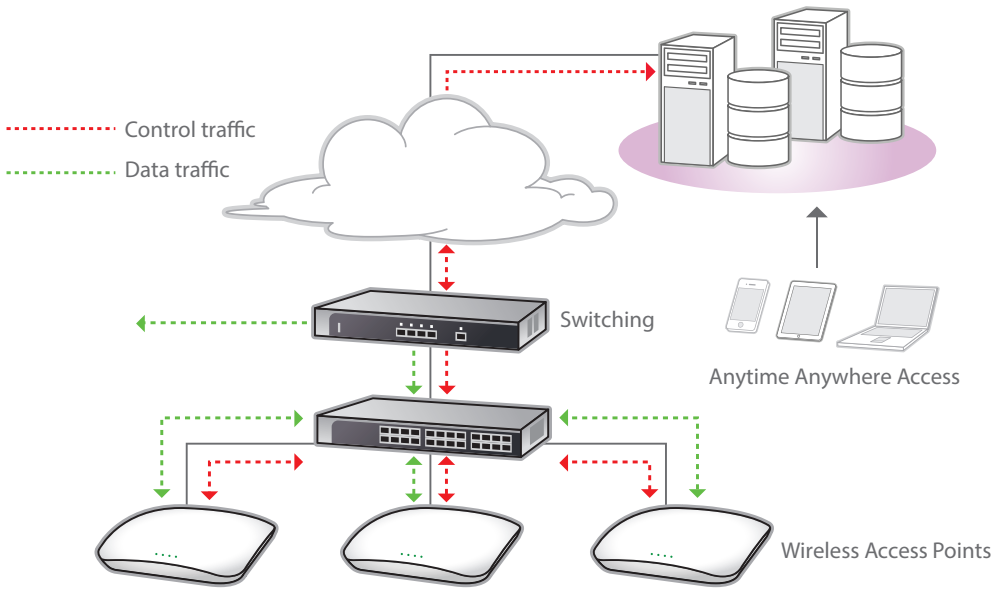
NETGEAR follows strict rule for privacy of personal data storage. By implementing the Safe Harbor rule, NETGEAR guarantees that all data are securely and privately maintain with no possibility of offering data to other third parties under the strictest guideline.

US-EU Safe Harbor is a streamlined process for US companies to comply with the EU Directive 95/46/EC on the protection of personal data. Intended for organizations that store customer data, the Safe Harbor Principles are designed to prevent accidental information disclosure or loss.

Encrypted Management Architecture

Control traffic between Business Central Wireless Manager and the access points is conducted through a secured tunnel. The access point verifies the authenticity of the cloud management system using a X.509 certificate. The authenticated connection is encrypted with 128-bit encryption using Advanced Encryption System (AES). The connection uses TLS 1.2 without SSL fallback. In addition, the data transmitted through this tunnel does not involve client data traffic.

Features



The above figure shows how Business Central would be deployed in a typical network. All data traffic flows directly from the AP's to the access wired network (as shown by the green line) while the control and monitoring traffic flows between the AP's and the cloud management platform (as shown by the red line). This approach allows user data to be quickly routed via the most efficient path to the Internet. Furthermore, any additional security treatment of the data path can be implemented directly on the various models of the NETGEAR switching portfolio.

Flexible Deployment Model

The tunnels between the Business Central Wireless Manager and the AP's are initiated by the AP's and not by the Cloud Management System, thereby ensuring that the organization's firewall will not need to have a port open on inbound connections. This approach ensures that the deployment can be easily supported in all network topology, including a NATted environment where the AP's are located behind a firewall and/or a branch gateway such as DSL or cable modem.

Redundancy and High Availability

Multiple geographically distributed data centers are used to host the Cloud Management System, thereby ensuring that the management system continues to function even in the event of a catastrophic failure of one data center.

Since the Business Central Wireless Manager is out of band for all data traffic, in the event that the organization's link to the Internet is interrupted, client data traffic will continue to flow normally — only configuration and administrative changes are temporarily impacted during an Internet connection outage. The system is automatically updated after the restoration of the Internet link.

Simplified Deployment

The provisioning of a wireless network just requires the deployment of supported access points — with setup and ongoing management undertaken inside the cloud management platform. Sizing, installation, configuration, and maintenance of a controller for management or traffic control plane is eliminated. Additional re-sizing of a controller when AP deployments grow is also eliminated.

Features

Single Sign-On Integration with MyNetgear.com portal

Leveraging a common database, namely the NETGEAR Support portal, customers now can have a single database repository for all NETGEAR products. From the MyNetgear.com portal, users can get information about the latest available firmware, FAQ, knowledge database, and customized views with information for all of the NETGEAR products that the user owns. The user does not need to remember multiple logins and passwords, and can now enjoy the simplicity of one log-on profile from a single portal page. The same logon credentials are used to access associated Business Central services.

Minimal IT Administration

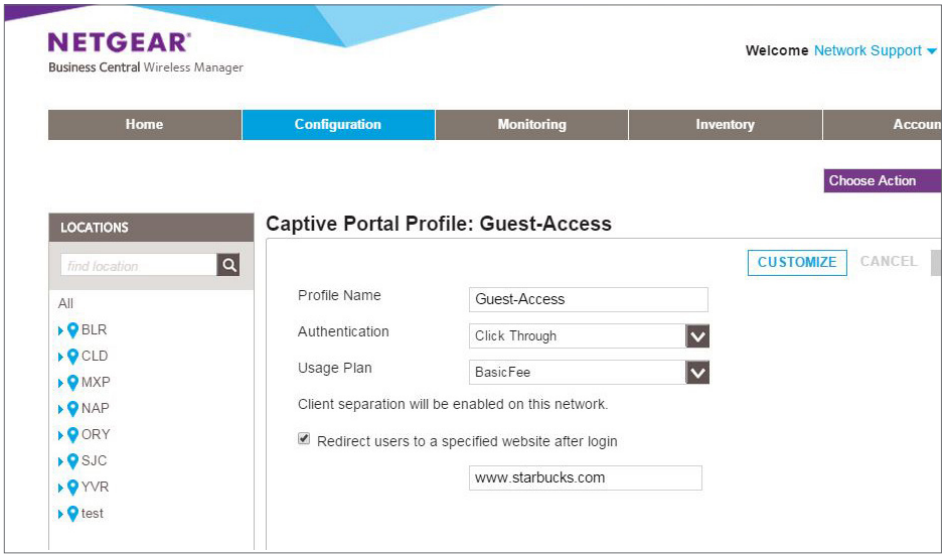
Because the Cloud Management System is hosted by NETGEAR (through cooperation with Amazon), updates and upgrades to the software are completely managed by NETGEAR during scheduled maintenance windows and are transparent to the organization's IT staff. Firmware updates of the wireless APs under cloud management are also conducted by NETGEAR , making time-intensive infrastructure maintenance updates a thing of the past.

Cost Effective Centralized Licensing Framework

As part of Business Central flexible licensing scheme, customers can not only purchase licenses for the number of APs that need to be supported, but also can adjust the number of licenses purchased based on the time that customers plan to manage the AP's. This two dimensional model (time and number of AP's) provides a totally flexible pay as you go model to suit customer requirements.

Robust Wireless Security

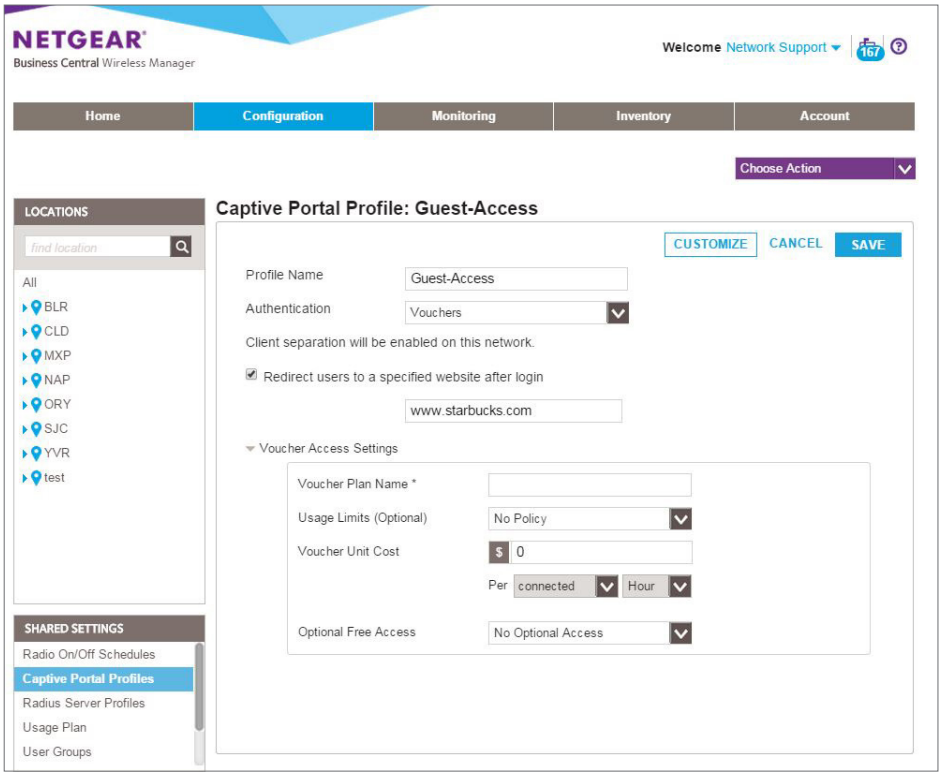
With identity-based security features such as support for RADIUS, Active Directory and internal or external AAA server, Business Central Wireless Manager truly unifies wired and wireless access without compromising on security. From the configuration menu of Business Central, the user can configure various wireless security settings such as WPA, WPA2, ACLs, radio parameters and push the settings to selected access points.



Features

Guest Access, Captive Portal and Logging

Guest access allows restricted access to the network, using an integrated captive portal. Four methods of entry are provided (Click-thru, Click-thru with email, Cloud AAA, and Voucher). **Click-Thru** guest access requires no authentication for the user to simply click through to access the wireless network. **Click-Through with Email** requires customers to enter the user email address to access the network. **Cloud AAA** requires users to enter username and password pairs for authentication prior to log in to the wireless network. **Voucher** option allows the premise to charge access to use the wireless network based on fee and/or time basis.



Dynamic RF management

Business Central Wireless Manager provides automatic control of access points' transmit power and channel allocation to ensure optimal coverage by minimizing channel interferences. Business Central Wireless Manager performs scheduled automatic channel allocation to deliver an enterprise class reliable wireless experience.

Client Load Balancing

Business Central Wireless Manager performs automatic load balancing of clients across access points to ensure even distribution of the traffic amongst the deployed APs.

Technical Features

RF MANAGEMENT	
Automatic Channel Allocation	• Automatic channel distribution to minimize interferences • Auto-channel allocation taking into consideration of the environment, interferences, traffic load and neighboring AP • Modifiable list of corporate channels to be used • Scheduled mode for Auto-channel allocation • Automatic mode in case of high level of interferences available
Automatic Power Control	• Optimum transmit power determination based on coverage requirements • Automatic power control mode available • Neighborhood scan of RF environment to minimize neighboring AP interference and leakage accross floors
Load Balancing	• APs load monitoring and overloading prevention • Clients redirection to lightly loaded neighboring APs
QUALITY OF SERVICE	
WMM Quality of Service	WMM (802.11e) prioritizes traffic for both upstream traffic from the stations to the Access Points (station EDCA parameters) and downstream traffic from the Access Points to the client stations (AP EDCA parameters)
WMM Queues in decreasing order of priority	• Voice: The highest priority queue with minimum delay, which makes it ideal for applications like VoIP and streaming media • Video: The second highest priority queue with low delay is given to this queue. Video applications are routed to this queue • Best Effort: The medium priority queue with medium delay is given to this queue. Most standard IP application will use this queue • Background: Low priority queue with high throughput. Applications, such as FTP, which are not time-sensitive but require high throughput can use this queue
WMM Power Save option	WMM Power Save helps conserve battery power in small devices such as phones, laptops, PDAs, and audio players using IEEE 802.11e mechanisms
WIRELESS SECURITY	
Client Authentication Protocols	• Open, WEP, WPA/WPA2-PSK • 802.11i/WPA/WPA2 Enterprise with standard interface to external AAA / RADIUS Server
Distinct AAA Server per location	Yes
RADIUS Accounting Protocol	Per Client tracking for: • Bytes Tx/Rx • Login/Logout Time
Integrated AAA Server	Local Database Authentification
Guest Access	• Click-Thru • Click-Throu with email • Cloud AAA • Voucher
Captive Portal	Configurable Portal page, including image files
Rogue Access Points*	• Rogue AP definition: AP with radio SSID oberved by any of the Managed AP and seen transmitting on same L2 wired network • Detection and Mapping of up to 512 Rogue APs

Technical Features

WIRELESS NETWORK MONITORING	
Monitoring Summary	Summary of the Managed Access Points status, rogue Access Points detected, Wireless stations connected
Managed Access Points	APs status for the Managed Access Points and details that includes configuration settings, current Wireless settings, current Clients and detailed Traffic statistics
Rogue Access Points	• Rogue Access Points Reported • Rogue Access Points in same channel • Rogue Access Points in interfering channels
Wireless Clients	• Clients statistics and details per AP, per SSID, per location • Black listed Clients, Roaming Clients
Wireless Network Usage	Network Usage Statistics display plots of average received/transmitted network traffic per Managed Access Point. Three different plots show Ethernet, Wireless 802.11 b/bg/ng and 802.11 a/na mode traffic separately

ORDERING INFORMATION	
SKU	**Description**
WM1AP1YL-10000S	Business Central Wireless Manager for managing 1 AP 1 year
WM1AP3YL-10000S	Business Central Wireless Manager for managing 1 AP 3 years
WM10AP1YL-10000S	Business Central Wireless Manager for managing 10 APs 1 year
WM10AP3YL-10000S	Business Central Wireless Manager for managing 10 APs 3 years
WM50AP1YL-10000S	Business Central Wireless Manager for managing 50 APs 1 year
WM50AP3YL-10000S	Business Central Wireless Manager for managing 50 APs 3 years

* This product comes with a limited warranty that is valid only if purchased from a NETGEAR authorized reseller, and modifications to product may void the warranty; covers hardware, fans, and internal power supplies—not software or external power supplies; see http://www.netgear.com/about/warranty/ for details. Lifetime technical support includes basic phone support for 90 days from purchase date and lifetime online chat support when purchased from a NETGEAR authorized reseller.

NETGEAR, the NETGEAR Logo, and ProSAFE are trademarks of NETGEAR, Inc. in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Information is subject to change without notice. © 2015 NETGEAR, Inc. All rights reserved.

D-BCentral-1